IN THE CLAIMS:

1-76. (Cancelled)

77. (New) A file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext, the file encryption apparatus comprising:

a portable key storage medium storing key information;

a memory unit storing a plaintext;

a file key generating unit operable to generate an original file key;

a text encrypting unit operable to generate a ciphertext by encrypting the plaintext stored in the memory unit using the original file key, and write the generated ciphertext into the memory unit; and

a key encrypting unit operable to generate a first encrypted file key by encrypting the original file key using a first password, generate a second encrypted file key by encrypting the original file key using the stored key information, and write the generated first and second encrypted file keys into the memory unit.

78. (New) The file encryption apparatus of Claim 77 further comprising:

a registration unit operable to receive an inputted password, generate an encrypted password by encrypting the inputted password using the stored key information, and write the generated encrypted password into the memory unit,

wherein the key encrypting unit further generates the first password by decrypting the encrypted password using the stored key information.

79. (New) The file encryption apparatus of Claim 78, wherein

the registration unit further receives an inputted user identifier for identifying a user, and writes the generated encrypted password and the inputted user identifier in association with each other into the memory unit, and

the key encrypting unit further receives the inputted user identifier, and decrypts the encrypted password associated with the user identifier.

80. (New) The file encryption apparatus of Claim 77, wherein

the key encrypting unit receives, one at a time, an instruction to generate the first encrypted file key and an instruction not to generate the first encrypted file key, and upon receiving the instruction to generate the first encrypted file key, generate the first encrypted file key, and upon receiving the instruction not to generate the first encrypted file key, inhibit the first encrypted file key from being generated and written into the memory unit.

81. (New) The file encryption apparatus of Claim 78, wherein

the registration unit further writes the generated encrypted password into the memory unit, wherein

the key encrypting unit further generates the first password by decrypting the encrypted password using the key information,

the registration unit further writes authentication information in association with the encrypted password, into the memory unit,

the key encrypting unit further checks, using the authentication information, whether or not the encrypted password has been altered, when the encrypted password is decrypted, and

the key encrypting unit further writes pieces of authentication information respectively in association with the first encrypted file key, the second encrypted file key, and the ciphertext, into the memory unit.

82. (New) The file encryption apparatus of Claim 78, wherein

the registration unit writes the encrypted password into the portable key storage medium, in place of into the memory unit, and

the key encrypting unit decrypts the encrypted password stored in the portable key storage medium.

83. (New) The file encryption apparatus of Claim 78, wherein

the registration unit further receives an inputted new password, generates a new encrypted password by encrypting the inputted new password using the stored key information, and writes the generated new encrypted password into the memory unit, and

the key encrypting unit further generates a file key by decrypting the second encrypted file key using the stored key information, generates a new first encrypted file key by encrypting the file key using the new password, and writes the new first encrypted file key in place of the first encrypted file key, into the memory unit.

84. (New) The file encryption apparatus of Claim 83, wherein

the registration unit further receives an inputted user identifier for identifying a user,

the key encrypting unit further writes the user identifier in association with the ciphertext, the first encrypted file key, and the second encrypted file key, into the memory unit, and

the key encrypting unit retrieves the second encrypted file key associated with the user identifier, and decrypts the retrieved second encrypted file key.

85 (New) The file encryption apparatus of Claim 83, wherein

the key encrypting unit further writes encryption information in association with the ciphertext. the first encrypted file key, and the second encrypted file key, into the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the key encrypting unit retrieves the second encrypted file key associated with the encryption information, and decrypts the retrieved second encrypted file key.

86. (New) The file encryption apparatus of Claim 83, wherein

the registration unit further receives an inputted user identifier for identifying a user,

the key encrypting unit further writes the user identifier in association with a file identifier for identifying the ciphertext, the first encrypted file key and the second encrypted file key, as a unified file, into the memory unit, and

the key encrypting unit extracts the file identifier that is associated with the user identifier from the unified file, identifies the second encrypted file key from the extracted file identifier, and decrypts the identified second encrypted file key.

87. (New) The file encryption apparatus of Claim 83, wherein

the key encrypting unit further writes encryption information in association with a file identifier for identifying the ciphertext, the first encrypted file key and the second encrypted file key, as a unified file, into the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the key encrypting unit extracts the file identifier that is associated with the encryption information from the unified file, identifies the second encrypted file key from the extracted file identifier, and decrypts the identified second encrypted file key.

88. (New) The file encryption apparatus of Claim 77 further comprising;

a deleting unit operable to delete the second encrypted file key from the memory unit.

89. (New) The file encryption apparatus of Claim 78, wherein

the portable key storage medium stores new key information in place of the stored key information,

the registration unit receives the inputted password and decrypts the received password using the new key information to generate a new encrypted password, and writes the generated new encrypted password over the encrypted password in the memory unit, and

the key encrypting unit decrypts the first encrypted file key using the password to generate a file key, encrypts the file key using the new key information to generate a new second encrypted file key, and writes the new second encrypted file key over the second encrypted file key in the memory unit.

90. (New) The file encryption apparatus of Claim 89, wherein

the registration unit further receives an inputted user identifier for identifying a user,

the key encrypting unit further writes the user identifier in association with the ciphertext, the first encrypted file key, and the second encrypted file key, into the memory unit, and

the key encrypting unit retrieves the first encrypted file key associated with the user identifier, and decrypts the

retrieved first encrypted file key.

91. (New) The file encryption apparatus of Claim 89, wherein

the key encrypting unit further writes encryption information in association with the ciphertext the first encrypted file key, and the second encrypted file key, into the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the key encrypting unit retrieves the first encrypted file key associated with the encryption information, and decrypts the retrieved first encrypted file key.

92. (New) The file encryption apparatus of Claim 89, wherein

the registration unit further receives an inputted user identifier for identifying a user,

the key encrypting unit further writes the user identifier in association with a file identifier for identifying the ciphertext, the first encrypted file key and the second encrypted file key, as a unified file, into the memory unit, and

the key encrypting unit extracts the file identifier that is associated with the user identifier from the unified file, identifies the first encrypted file key from the extracted file identifier, and decrypts the identified first encrypted file key.

93. (New) The file encryption apparatus of Claim 89, wherein

the key encrypting unit further writes encryption information in association with a file identifier for identifying the ciphertext, the first encrypted file key and the second encrypted

file key, as a unified file, into the memory unit, the encryption information indicating that the plaintext has been encrypted, and

the key encrypting unit extracts the file identifier that is associated with the encryption information from the unified file, identifies the first encrypted file key from the extracted file identifier, and decrypts the identified first encrypted file key.

94. (New) A file decryption apparatus that decrypts a ciphertext, the file decryption apparatus comprising:

a portable key storage medium storing key information;

a memory unit storing the ciphertext, the first encrypted file key, and the second encrypted file key that are generated by the file encryption apparatus defined in Claim 77;

a first key obtaining unit operable to generate a first decrypted file key by decrypting the first encrypted file key using a second password;

a second key obtaining unit operable to generate a second decrypted file key by decrypting the second encrypted file key using the stored key information;

a switch unit operable to switch between the first key obtaining unit and the second key obtaining unit;

a decrypting unit operable to generate a decrypted text by decrypting the ciphertext using either the first decrypted file key generated by the first key obtaining unit or the second decrypted file key generated by the second key obtaining unit; and

a deleting unit operable to delete either the first decrypted file key or the second decrypted file key.

95. (New) The file decryption apparatus of Claim 94, wherein

the memory unit further stores pieces of authentication information respectively in association with the first encrypted file key, the second encrypted file key, and the ciphertext,

each of the first key obtaining unit and the second key obtaining unit further checks, using a piece of authentication information associated with the first encrypted file key or the second encrypted file key, whether or not the first encrypted file key or the second encrypted file key has been altered, when the first encrypted file key or the second encrypted file key is decrypted, and

the decrypting unit checks, using a piece of authentication information associated with the ciphertext, whether or not the ciphertext has been altered, when the ciphertext is decrypted.

96. (New) The file decryption apparatus of claim 94 further comprising:

a matching unit operable to receive an inputted third password, generate a first file key by decrypting the first encrypted file key using the third password, generate a second file key by decrypting the second encrypted file key using the stored key information, judges whether or not the first file key matches the second file key, and recognize an error if the first file key does not match the second file key.

97. (New) A file management apparatus that encrypts a plaintext to generate a ciphertext, stores the ciphertext, and decrypts the ciphertext, the file management apparatus comprising:

a portable key storage medium storing key information;

a memory unit storing a plaintext;

a file key generating unit operable to generate an original file key;

a text encrypting unit operable to generate a ciphertext by encrypting the plaintext stored in the memory unit using the original file key, and write the generated ciphertext into the memory unit;

a key encrypting unit operable to generate a first encrypted file key by encrypting the original file key using a first password, generate a second encrypted file key by encrypting the original file key using the stored key information, and write the generated first and second encrypted file keys into the memory unit;

a first key obtaining unit operable to generate a first decrypted file key by decrypting the first encrypted file key using a second password;

a second key obtaining unit operable to generate a second decrypted file key by decrypting the second encrypted file key using the stored key information.

a switch unit operable to switch between the first key obtaining unit and the second key obtaining unit;

a decrypting unit operable to generate a decrypted text by decrypting the ciphertext using either the first decrypted file key generated by the first key obtaining unit or the second decrypted file key generated by the second key obtaining unit; and

a deleting unit operable to delete either the first decrypted file key or the second decrypted file key.

98. (New) A file encryption method for use in a file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext, the file encryption apparatus including:

a portable key storage medium storing key information; and

a memory unit storing a plaintext,

the file encryption method comprising the steps of generating an original file key;

generating a ciphertext by encrypting the plaintext stored in the memory unit using the original file key, and writing the generated ciphertext into the memory unit; and

generating a first encrypted file key by encrypting the original file key using a first password, generating a second encrypted file key by encrypting the original file key using the stored key information, and writing the generated first and second encrypted file keys into the memory unit.

99. (New) A computer program for encrypting files, for use in a file encryption apparatus that encrypts a plaintext to generate a ciphertext and stores the ciphertext, the file encryption apparatus including:

a portable key storage medium storing key information; and

a memory unit storing a plaintext,

the computer program comprising the steps of:

generating an original file key;

generating a ciphertext by encrypting the plaintext stored in the memory unit using the original file key, and writing the generated ciphertext into the memory unit; and

generating a first encrypted file key by encrypting the original file key using a first password, generating a second encrypted file key by encrypting the original file key using the stored key information, and writing the generated first and second encrypted file keys into the memory unit.

100. (New) A file decryption method for use in a file decryption apparatus that decrypts a ciphertext, the file decryption apparatus including:

a portable key storage medium storing key information; and

a memory unit storing the ciphertext, the first encrypted file key, and the second encrypted file key that are generated by the file encryption apparatus defined in Claim 77,

the file decryption method comprising the steps of:

generating a first decrypted file key by decrypting the first encrypted file key using a second password;

generating a second decrypted file key by decrypting the second encrypted file key using the stored key information;

switching between the first decrypted file key generating step and the second decrypted file key generating step;

generating a decrypted text by decrypting the ciphertext using either the first decrypted file key generated by the first decrypted file key generating step or the second decrypted file key generated by the second decrypted file key generating step; and

deleting either the first decrypted file key or the second decrypted file key.

101. (New) A computer program for decrypting files, for use in a file decryption apparatus that decrypts a ciphertext, the file decryption apparatus including:

a portable key storage medium storing key information; and

a memory unit storing the ciphertext, the first encrypted file key, and the second encrypted file key that are generated by the file encryption apparatus defined in Claim 77,

the computer program comprising the steps of:

generating a first decrypted file key by decrypting the first encrypted file key using a second password;

generating a second decrypted file key by decrypting the second encrypted file key using the stored key information;

switching between the first decrypted file key generating step and the second decrypted file key generating step;

generating a decrypted text by decrypting the ciphertext using either the first decrypted file key generated by the first decrypted file key generating step or the second decrypted file key generated by the second decrypted file key generating step; and

deleting either the first decrypted file key or the second decrypted file key.